Netigy℠

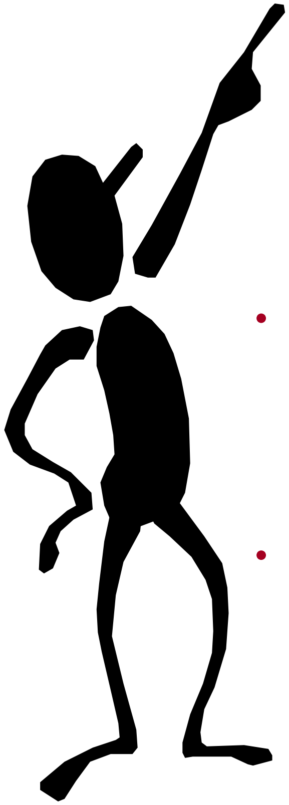
Operational Computer Forensics – The New Frontier

Michael J. Corby, CCP, CISSP

Vice President,

Netigy Corporation

Abstract



- The industry has, at long last, accepted Computer Security as a key component of any organization's operating and strategic plan. There can be no doubt that preventing unwanted access to systems, files and the computer environment is a good thing. Furthermore, the accurate and data storage, retrieval and processing is crucial for success. But what happens if somewhere, somehow a chink in the armor is revealed. Do you have the procedures in place to identify that an "event" has occurred, how you can prevent future occurrences and how the situation was caused. Tracking the source of the problem and in some cases, establishing corrective measures and providing reliable and usable evidence for legal proceedings (if necessary) can pose a new challenge. Computer forensics is a new specialty that can identify the proper procedures for collecting evidence in a manner suitable for use in apprehending and prosecuting security violators.

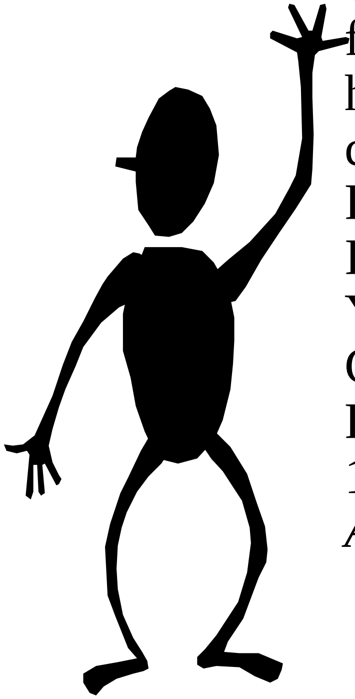
- The first part of this session will identify some of key elements in building an effective Computer Forensics program within the Computer Security practice area. Many areas will be covered including procedures, career issues, legal processes and financial justification.

- The second part will focus on specific ways to configure clients and servers in a LAN environment to facilitate forensic data collection and establish proper evidence collection procedures. Platforms covered will include: Novell and Windows/NT servers; DOS, Windows 3.x, 95, 98 and NT clients. Attendees will review a checklist of parameters to specify and methods to use that maximize data collection and preservation.

Netigy

About the Speaker:

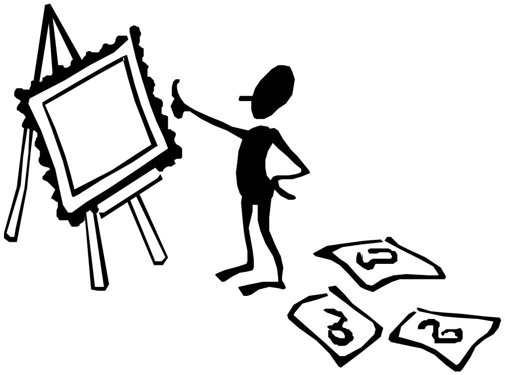
- Mr. Corby is Vice President of the Global Security Practice of Netigy Corporation (previously known as: Enterprise Networking Systems, Inc.). He was formerly CEO and Consulting Director for M Corby & Associates, Inc. a US Consultancy founded in 1989.   He has been an IT Professional for over 30 years specializing in systems technology management and computer security. As a Technology Specialist, Systems Manager and CIO for large international corporations, and as Consulting Director of hundreds of Systems and Technology projects for several diverse companies, he has put many theories and creative ideas into practice. Prior to his term as the Consulting Director for M Corby & Associates, Inc., he was practice director for the IT Consulting Practice of Ernst & Young, CIO for a division of Ashland Oil and the Bain & Company Consulting Group. He is a Certified Information Systems Security Professional (CISSP) and Certified Computer Professional (CCP). In 1994, the Computer Security Institute awarded Mike the *Lifetime Achievement Award*



Netigy

Objectives

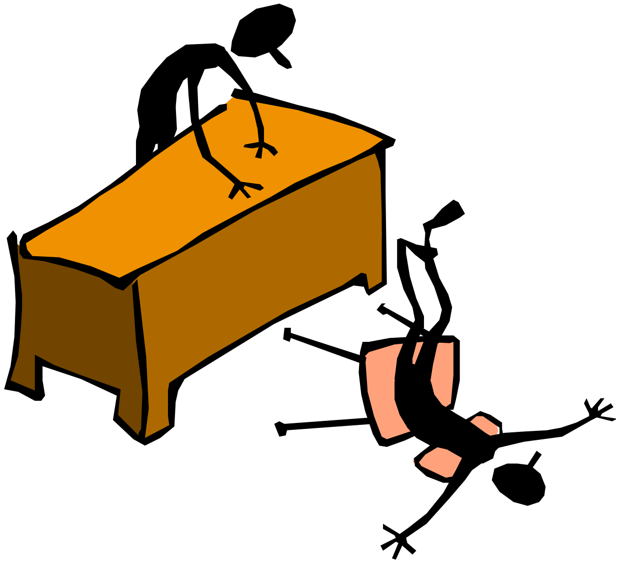
- After this workshop, you should:
  - understand the basics of computer forensics and where they can be applied
  - understand the scope and relevance of operational forensics
  - learn some techniques for conducting a computer forensics analysis
  - build a strategy for incorporating operational forensics into your computer security practice



Netigy

Agenda

- Introduction
- The State of the Industry: 2000 and beyond
- Event identification
- Prevention/Mitigation
- Elements of Forensics
- What is “operational” Forensics
- Platform Specifics
- Organizational Specifics
- Summary - Q/A



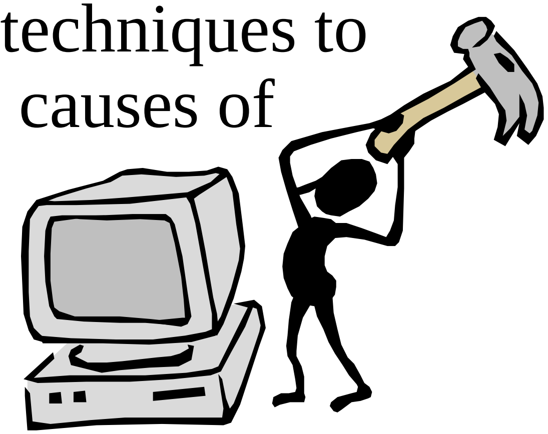
Introduction

- **What is computer forensics anyway?**

  The application of computer investigations and analysis techniques in the interests of determining potential legal evidence. Computer specialists can draw on an array of methods for discovering deleted, encrypted, or damaged file information (Robbins, 1997).

- **What is “Operational Forensics”**

  The application of computer forensics techniques to identify the occurrence and underlying causes of observed computer-based events.



Netigy

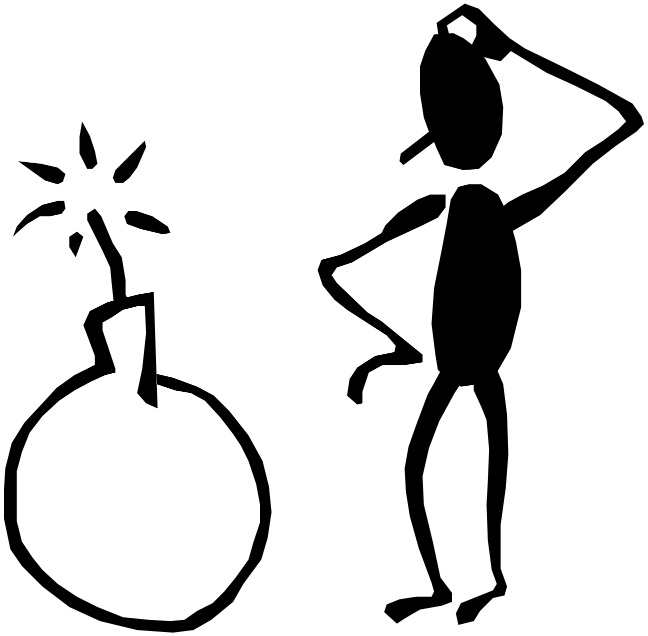
State of the Industry: 2000 & beyond

- Accountability
- Responsiveness
- Privacy
- Employee/employer “Rights and Obligations”
- The dot-com society and its effects

Netigy

Event Identification

- Human Behavior
  - blackmail
  - extortion
  - disgruntled employee
  - obtuse behavior
  - “dropping the dime”
  - sabotage/corporate espionage



Event Identification (2)

- Physical Behavior
  - flood, fire, earthquake, etc.
  - mechanical failures
  - physical access prohibited
  - theft/damage

Netigy

Event Identification (3)

- Organizational Issues
  - operating system upgrade
  - new hardware
  - new software

Event Identification (4)

- Operational Issues
  - disk failure
  - backup
  - virus
  - accidental deletions (oops!)
  - overwrite

Prevention/Mitigation

- Procedural
- Disaster recovery plan
- planning by project manager
- purchasing hardware & software (data security)

Netigy

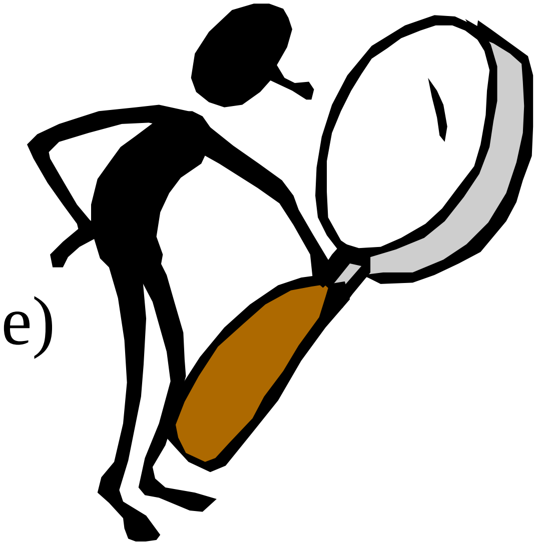
Indirect Results of these Events

- Loss of service
- Discontinuity of reporting
- Profit loss

Netigy

Elements of Forensics

- Recovery
  - evidence preservation
  - damage control
  - system restoration
- Causation (problem source)
- Proof
  - evidence analysis



Netigy

Objectives of Forensics

Traditional

- Prove it in court (legal)

Operational

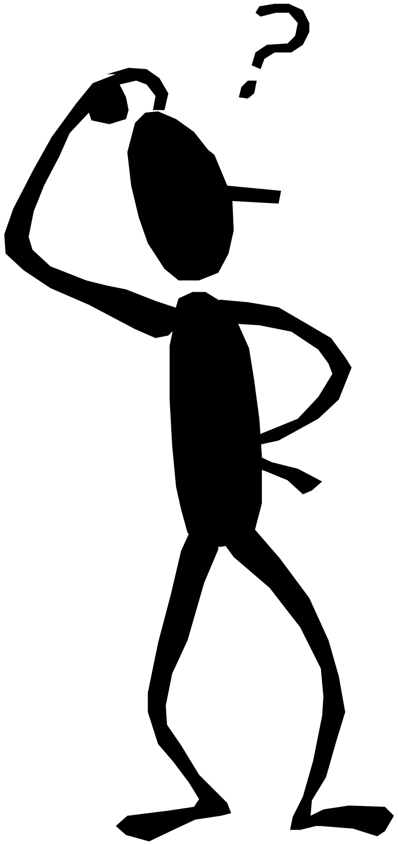
- Prove it to prevent future incidents
- Prove it to define performance benchmarks
- Prove it to improve QoS

Netigy

Financial Implications

- Insurance for theft/loss
- E & O (???)
- Purchase of extra hardware for incident potential and response
- Risk to business
- Loss/new business (e.g., no controls = loss of clientele and sound controls = increase in clientele)

Netigy | Q & A



Netigy

Summary

- **Computer Forensics is an important element of <u>any</u> Security Program.**
- **Problem recovery may be quicker if reactive, but may not yield stability.**
- **Weigh the importance of 3 factors:**
  - **Restoration**
  - **Prevention**
  - **Prosecution**
- **As with anything else: Stay Current!**

Netigy℠

Platform Architecture I

Windows NT

Windows NT Workstation Preparation Checklist[1]

Note: *The Windows NT workstation platform is designed to be a secure desktop environment, but only under well established conditions. The focus of preparation of a Windows NT workstation is directed toward the environment to which the system user (authorized or unauthorized) has been advised of their responsibilities for "official use" and password confidentiality, and also on the technical implementation of the operating software for evidence collection and non-repudiation (inability of the suspect to deny actions).*

A. Legal Notice

1. ***1. Has a legal notice of the company policy & practice been put in place?***
2. ***Has the logon dialog box been enabled?***
3. ***Is there a password policy in place to prevent users from sharing their passwords?***

B. Monitoring and Viewer programs

1. ***Performance Monitor***
    a. ***Is this utility used to gather, analyze, and graphically display critical information about the system?***
    b. ***Is Chart View used? Alert View? Log View? Report View?***
        - What objects are tracked under each?
        - Why are these objects tracked?
        - On what frequency is each tracked?
        - For Alert View, what are the threshold values (i.e., the levels that must be reached in order to send out an alert)?
        - Who receives the alerts?
        - For Log View and Report View, are critical logs updated manually or periodically? If periodically, what are the time intervals for updates?
2. ***Network Monitor***
    a. ***Is this utility being used to monitor network traffic?***
    b. ***If so, on what frequency is this utility used to monitor traffic to and from the server?***
    c. ***Which network addresses, protocols, and protocol properties are monitored?***
    d. ***What triggers (i.e., conditions that must be met before an action occurs) have been set for what conditions?***
    e. ***Are reviews conducted for identifying unauthorized copies of Network Monitor running on the network? Investigate who else on the network has installed and is using Network Monitor.***
    f. ***Are any third-party network monitoring tools used?***
3. ***Event Viewer***

[1] James G. Jumes, Neil F. Cooper, Paula Chamoun & Todd M. Feinman. *Microsoft Technical Reference: Microsoft Windows NT 4.0 Security, Audit, and Control*. (Redmond, WA: Microsoft Press, 1999)

Netigy℠

Platform Architecture II

Windows 95/98

Windows 95/98 Workstation Preparation Checklist

Note: *The Windows 95 and Windows 98 platforms are not designed to be a secure desktop environment. Usage logs are not available in the native operating system and the FAT file system is not capable of restricting access by unauthorized individuals. Because of these restrictions non-repudiation (inability of the suspect to deny actions) isn't possible. Therefore, the focus of preparation on Windows 95/98 workstations is directed toward the environment to which the system user (authorized or unauthorized) has been advised of their responsibilities for "official use" and password confidentiality.*

A. User Security under Windows 95/98

1. ***Has a legal notice of the company policy & practice been put in place?***
2. ***Has the logon dialog box been enabled?***
3. ***Is there a password policy in place to prevent users from sharing their passwords?***

B. Workstation Security

1. ***Have the user profiles been configured according to the needs of each user?***
2. ***Has Policy Editor been installed to secure user profiles on the desktop?***
3. ***If the workstation uses a BIOS power on password, it is activated?***
4. ***Do cables or alarms physically secure workstations?***
5. ***Are removable media drives, such as floppy, removable hard drives, writable CD-ROM, and portable streaming tape units, available on workstations?***
6. ***Have floppy drives been disabled?***
7. ***Have compact disk drives been disabled?***
8. ***Do workstations contain modems that are connected to telephone lines?***
9. ***If workstations contain modems that are connected to telephone lines, is remote dial-in restricted or allowed?***
10. ***If workstations contain modems that are connected to telephone lines, is the Callback option enabled?***
11. ***Are any of the telephone lines restricted to “dial out” only by the Telephone Company?***

C. Network Access Points

1. ***Are network access points restricted to active computers only?***
2. ***Are unused network access points physically secured through locks or disconnected?***

D. Protocols

1. ***What protocols have been deployed on your network and why have they been selected?***
2. ***TCP/IP***
   a. ***Are simple TCP/IP services installed?***
   b. ***What are the TCP/IP settings?***

Netigy℠

Platform Architecture III

DOS/Windows 3.1x

Windows 3.1x/DOS Workstation Preparation Checklist

Note: *The DOS and 16 bit Windows platforms are not designed to be a secure desktop environment. Usage logs are not available in the native operating system and the FAT file system is not capable of restricting access by unauthorized individuals. Because of these restrictions non-repudiation (inability of the suspect to deny actions) isn't possible. Therefore, the focus of preparation on these workstations is directed toward the environment to which the system user (authorized or unauthorized) has been advised of their responsibilities for "official use" and password confidentiality.*

A. Legal Notice

1. Has a legal notice of the company policy & practice been put in place?

2. Is there a password policy in place to prevent users from sharing their passwords?

B. Workstation Security

1. If the workstation uses a BIOS power on password, it is activated?

2. Has the user desktop been configured according to the needs of each user?

***3. If possible, is the user prevented from changing the prescribed desktop settings by inserting the following values in the* "progman.ini" settings of the Windows directory?**

```
[restrictions] section
        NoRun=1              (Disables the "run" command)
        NoClose=1            (Disables the "Exit Windows" option)
        NoSaveSettings=1     (Disables the "saves settings on exit" option)
        NoFileMenu=1         (Removes access to the File menu)
        EditLevel=n          (see below)
```

0 allows the user to make any change. (This is the default.)

1 prevents the user from creating, deleting, or renaming groups. If you specify this value, the New, Move, Copy, and Delete commands on the File menu are not available when a group is selected.

2 sets all restrictions in EditLevel= 1, plus prevents the user from creating or deleting program items. If you specify this value, the New, Move, Copy, and Delete commands on the File menu are not available.

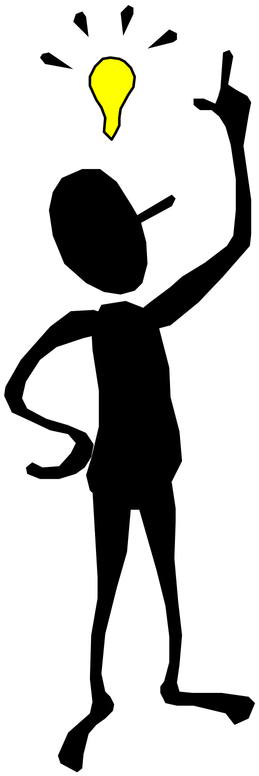
3 sets all restrictions in EditLevel= 2, plus prevents the user from changing command lines for program items. If you specify this value, the text in the Command Line box in the Properties dialog box cannot be changed.

4 sets all restrictions in EditLevel= 3, plus prevents the user from changing any program item information. If you specify this value, none of the areas in the Properties dialog box can be modified. The user can view the dialog box, but all of the areas are dimmed.

4. Do cables or alarms physically secure workstations?

Netigy

Comments and Observations



Netigy | Bibliography of References

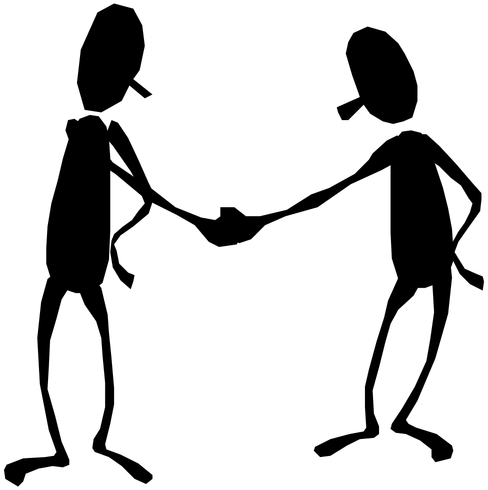
- Burton, R.F. (1996). “Searching for Fraud Behind the Screens,” *The White Paper*, Vol.. 10 (2), The Association for Certified Fraud Examiners
- Forgione, D. (1994). “Recovering “Lost” Evidence from a Microcomputer,” *The White Paper*, Vol.. 8(3), The Association for Certified Fraud Examiners
- Clede, Bill (1993). Investigating Computer Crime is Every Department’s Concern, *Law and Order*, July 1993. Available for FTP at: `ourworld.compuserve.com/homepages/billc/compcrim.htm`
- Conly, C.H. & McEwen, J.T. (1990). Computer Crime: The New Crime Scene. NIJ Reports No. 218, National Institute of Justice, Office of Justice Programs, U.S. Department of Justice
- Farwell, W. L. (1997). “Stand-alone PC Examinations: Some Basic Forensic Guidelines,” High Technology Crime Investigation Association Newsletter, New England Chapter, Vol. 2(1).

Netigy

Bibliography (2)

- Howell, F.J., Spernow, W. and Farwell, W.L. (1998). “Computer Search & Seizure and Computer Forensics,” HTCIA Training Seminar in Boston, MA, April 1998.
- Robbins, J. (1998). An Explanation of Computer Forensics by Judd Robbins. Available at `knock-knock.com`
- Rosenblatt, K.S. (1995). *High Technology Crime: Investigating Cases Involving Computers.* San Jose: KSK Publications

If You Would Like More:



Michael J. Corby, CCP, CISSP

Netigy Corporation
255 Park Avenue, 8th Floor
Worcester, MA 01609-1946 U.S.A.
Phone: 1 (508) 792-4321
Fax: 1 (508) 792-4327
Web: www.Netigy.com
E-Mail: mike.corby@netigy.com